S

www.archive.org
415.561.6767
415.840.0391 fax

mail:
Internet Archive
PO Box 29244
San Francisco, CA
94129-0244

ship:
Internet Archive
116 Sheridan Avenue
Presidio of San Francisco
San Francisco, CA 94129

AFFIDAVIT OF PAUL HICKMAN

1. I am the Office Manager at the Internet Archive, located at the Presidio of San Francisco, California. I make this declaration of my own personal knowledge.

2. The Internet Archive is a website that provides access to a digital library of Internet sites and other cultural artifacts in digital form. Like a paper library, we provide free access to researchers, historians, scholars, and the general public. The Internet Archive is affiliated with and receives support from various institutions, including the Library of Congress.

3. The Internet Archive has created a service known as the Wayback Machine. The Wayback Machine makes it possible to surf more than 55 billion pages stored in the Internet Archive's web archive. Visitors to the Wayback Machine can type in a URL (i.e., a website address), select a date range, and then begin surfing on an archived version of the Web. The links on the archived files, when served by the Wayback Machine, point to other archived files (whether HTML pages or images). If a visitor clicks on a link on an archived page, the Wayback Machine will serve the archived file with the closest available date to the originally requested page.

4. The Internet Archive receives data from third parties who compile the data by using software programs known as crawlers that surf the Web and automatically store copies of website files at certain points in time as they existed at that point in time. This data is donated to the Internet Archive, which preserves and provides access to it.

5. The Internet Archive assigns a URL on its site to the archived files in the format http://web.archive.org/web/[Year in yyyy][Month in mm][Day in dd][Time code in hh:mm:ss]/[Archived URL]. Thus, the Internet Archive URL http://web.archive.org/web/19970126045828/http://www.archive.org/ would be the URL for the record of the Internet Archive home page HTML file (http://www.archive.org/) archived on January 26, 1997 at 4:58 a.m. and 28 seconds (1997/01/26 at 04:58:28). Typically, a printout from a Web browser will show the URL in the footer. The date assigned by the Internet Archive applies to the HTML file but not to image files linked therein. Thus images that appear on the printed page may not have been archived on the same date as the HTML file. Likewise, if a website is designed with "frames," the date assigned by the Internet Archive applies to the frameset as a whole, and not the individual pages within each frame.

6. Attached hereto as Exhibit A are true and accurate copies of printouts of the Internet Archive's records of the HTML files archived from the URLs and the dates specified in the footer of the printout.

7. I declare under penalty of perjury that the foregoing is true and correct.

DATE: 4/17/06

Paul Forrest Hickman

Golden State Notary Acknowledgment Form

State of California
County of San Francisco } ss.

On April 17th before me, David Ryan

personally appeared Paul Forrest Hickman

personally known to me (or proved to me on the basis of satisfactory evidence) to be the person(s) whose name(s) is/are subscribed to the within instrument and acknowledged to me that he/she/they executed the same in his/her/their authorized capacity(ies), and that by his/her/their signature(s) on the instrument the person(s), or the entity upon behalf of which the person(s) acted, executed the instrument.

WITNESS my hand and official seal.

DAVID RYAN
COMM. # 1648329
NOTARY PUBLIC-CALIFORNIA
SAN FRANCISCO COUNTY
My Commission Expires
February 19, 2010

Signature of Notary

Affidavit Paul Hickman

Notes

Acknowledgment

Please provide information about the document that this form is attached to.
This is not required under California State notary public law.

 www.GoldenStateNotary.com (888) 263-1977

ISS_02125904

Scale Intrusion Detection for the Emerging Network Infrastructure

Objective

What. This three-year DARPA-funded project is to design and develop a software system for protecting against intruders from breaking into network routers, switches, and network management channels. The project is a joint collaboration between MCNC and North Carolina State University (NCSU).

Why. Given the increasing popularity of the Internet, intrusion incidents are becoming common events of life. Attacks on the network infrastructure has the potential of disrupting a large scale of information services on which the national defense and economy may depend. Despite the best efforts of the protocol designers, implementors, and system administrators, it is prudent to assume that attacks will occur and some, unfortunately, will succeed. Therefore, it is vitally important to develop means to automatically detect and respond to these attacks in order to maintain these critical information services.

Approach

In this project, we will design, implement, and integrate intrusion detection techniques based on statistical and logical analysis of network routing and management protocols to construct a scalable distributed intrusion detection system for the emerging internetwork environment. At the top level, the system consists of local detection subsystems and remote management application subsystems. The integration of these two subsystems will be mapped onto the SNMP standard management framework.

A local subsystem has three major components: rule-based prevention module, protocol-based detection module, and statistical analysis detection module. As a gate-keeper, the prevention module intercepts and filters all incoming packets according to a small set of rules. It conducts a quick check to see whether an incoming packet violate general security guidelines or special administrative security concerns. A second component of the system uses logical analysis of protocol operation. This technique detects intrusion by monitoring the execution of protocols in a router/switch and triggering an intrusion alarms when an anomalous state is entered. The statistical-based approach is founded on the contention that network routing and management protocols exhibit certain behavioral signatures. Any behavior deviating from the normal signature will be considered as an anomaly and appropriate alarms can be triggered.

The detection functions of a local subsystem are complementary in nature in terms of their capabilities and their response times. The rule and protocol-based approach is meant to analyze and detect known vulnerabilities. On the other hand, the statistical analysis is intended to uncover those attacks that cannot be prevented by a set of rules embedded in a rule-based component or cannot be detected by security analysis conducted through protocol-based approach. As far as response time is concerned, the statistical approach requires an observation window to determine whether the target is anomalous. The protocol-based and, especially, the rule-based mechanisms will be able to detect the targeted intrusions with relatively low latency.

For demonstration purposes, we will implement simple network management applications for accessing and coordinating local detection information. The choice of using SNMP as the information exchange

protocol was based on the fact that it is standardized and any other security applications based on SNMP may potentially interoperate with our system with relative ease.

To evaluate the system design and implementation, we will develop a set of attacks and use them to exercise our system by attacking nodes within a testbed network. These tests will allow us to measure the run-time overhead introduced by the intrusion detection system. After the validation process, we expect to deploy and evaluate the system in an operational network.

Related Information

- Project Viewgraph
- Architecture Design Report

• Contact: Y. Frank Jou; Email: jou@mcnc.org

MCNC
Post Office Box 12889
Research Triangle Park
North Carolina 27709-2889

Last Modified: April, 1997

Scalable Intrusion Detection for the Emerging Network Infrastructure

Objective

What. This three-year DARPA-funded project is to design and develop a software system for protecting against intruders from breaking into network routers, switches, and network management channels. The project is a joint collaboration between MCNC and North Carolina State University (NCSU).

Why. Given the increasing popularity of the Internet, intrusion incidents are becoming common events of life. Attacks on the network infrastructure has the potential of disrupting a large scale of information services on which the national defense and economy may depend. Despite the best efforts of the protocol designers, implementors, and system administrators, it is prudent to assume that attacks will occur and some, unfortunately, will succeed. Therefore, it is vitally important to develop means to automatically detect and respond to these attacks in order to maintain these critical information services.

Approach

In this project, we will design, implement, and integrate intrusion detection techniques based on statistical and logical analysis of network routing and management protocols to construct a scalable distributed intrusion detection system for the emerging internetwork environment. At the top level, the system consists of local detection subsystems and remote management application subsystems. The integration of these two subsystems will be mapped onto the SNMP standard management framework.

A local subsystem has three major components: rule-based prevention module, protocol-based detection module, and statistical analysis detection module. As a gate-keeper, the prevention module intercepts and filters all incoming packets according to a small set of rules. It conducts a quick check to see whether an incoming packet violate general security guidelines or special administrative security concerns. A second component of the system uses logical analysis of protocol operation. This technique detects intrusion by monitoring the execution of protocols in a router/switch and triggering an intrusion alarms when an anomalous state is entered. The statistical-based approach is founded on the contention that network routing and management protocols exhibit certain behavioral signatures. Any behavior deviating from the normal signature will be considered as an anomaly and appropriate alarms can be triggered.

The detection functions of a local subsystem are complementary in nature in terms of their capabilities and their response times. The rule and protocol based approach is meant to analyze and detect known vulnerabilities. On the other hand, the statistical analysis is intended to uncover those attacks that cannot be prevented by a set of rules embedded in a rule-based component or cannot be detected by security analysis conducted through protocol-based approach. As far as response time is concerned, the statistical approach requires an observation window to determine whether the target is anomalous. The protocol-based and, especially, the rule-based mechanisms will be able to detect the targeted intrusions with relatively low latency.

For demonstration purposes, we will implement simple network management applications for accessing and coordinating local detection information. The choice of using SNMP as the information exchange

protocol was based on the fact that it is standardized and any other security applications based on SNMP may potentially interoperate with our system with relative ease.

To evaluate the system design and implementation, we will develop a set of attacks and use them to exercise our system by attacking nodes within a testbed network. These tests will allow us to measure the run-time overhead introduced by the intrusion detection system. After the validation process, we expect to deploy and evaluate the system in an operational network.

Related Information

- Project Viewgraph (powerpoint)
- Architecture Design Report (postscript)
- Project Update Viewgraph (at SRI, July 97, powerpoint)
- Project Update Viewgraph (at Annapolis, MD, Feb. 98, powerpoint)

- Contact: Y. Frank Jou, Email: jou@mcnc.org

MCNC
Post Office Box 12889
Research Triangle Park
North Carolina 27709-2889

Last Modified: September 24, 1997

Scalable Intrusion Detection for the Emerging Network Infrastructure

Objective

What. This three-year DARPA-funded project is to design and develop a software system for protecting against intruders from breaking into network routers, switches, and network management channels. The project is a joint collaboration between MCNC and North Carolina State University (NCSU).

Why. Given the increasing popularity of the Internet, intrusion incidents are becoming common events of life. Attacks on the network infrastructure has the potential of disrupting a large scale of information services on which the national defense and economy may depend. Despite the best efforts of the protocol designers, implementors, and system administrators, it is prudent to assume that attacks will occur and some, unfortunately, will succeed. Therefore, it is vitally important to develop means to automatically detect and respond to these attacks in order to maintain these critical information services.

Approach

In this project, we will design, implement, and integrate intrusion detection techniques based on statistical and logical analysis of network routing and management protocols to construct a scalable distributed intrusion detection system for the emerging internetwork environment. At the top level, the system consists of local detection subsystems and remote management application subsystems. The integration of these two subsystems will be mapped onto the SNMP standard management framework.

A local subsystem has three major components: rule-based prevention module, protocol-based detection module, and statistical analysis detection module. As a gate-keeper, the prevention module intercepts and filters all incoming packets according to a small set of rules. It conducts a quick check to see whether an incoming packet violate general security guidelines or special administrative security concerns. A second component of the system uses logical analysis of protocol operation. This technique detects intrusion by monitoring the execution of protocols in a router/switch and triggering an intrusion alarms when an anomalous state is entered. The statistical-based approach is founded on the contention that network routing and management protocols exhibit certain behavioral signatures. Any behavior deviating from the normal signature will be considered as an anomaly and appropriate alarms can be triggered.

The detection functions of a local subsystem are complementary in nature in terms of their capabilities and their response times. The rule and protocol based approach is meant to analyze and detect known vulnerabilities. On the other hand, the statistical analysis is intended to uncover those attacks that cannot be prevented by a set of rules embedded in a rule-based component or cannot be detected by security analysis conducted through protocol-based approach. As far as response time is concerned, the statistical approach requires an observation window to determine whether the target is anomalous. The protocol-based and, especially, the rule-based mechanisms will be able to detect the targeted intrusions with relatively low latency.

For demonstration purposes, we will implement simple network management applications for accessing and coordinating local detection information. The choice of using SNMP as the information exchange

protocol was based on the fact that it is standardized and any other security applications based on SNMP may potentially interoperate with our system with relative ease.

To evaluate the system design and implementation, we will develop a set of attacks and use them to exercise our system by attacking nodes within a testbed network. These tests will allow us to measure the run-time overhead introduced by the intrusion detection system. After the validation process, we expect to deploy and evaluate the system in an operational network.

Related Information

- Project Viewgraph (powerpoint)
- Architecture Design Report (postscript)
- Project Update Viewgraph (powerpoint)
- Contact: Y. Frank Jou, Email: jou@mcnc.org

MCNC
Post Office Box 12889
Research Triangle Park
North Carolina 27709-2889

Last Modified: September 24, 1997

Scalable Intrusion Detection for the Emerging Network Infrastructure

ANR

MCNC

Scalable Intrusion Detection for the Emerging Network Infrastructure

Project Update

PP Presentation

PP Presentation

System Design:

System Design: Intercept. Mod.

PP Presentation

PP Presentation

PP Presentation

PP Presentation

PP Presentation

PP Presentation

PP Presentation

PP Presentation

PP Presentation

PP Presentation

PP Presentation

PP Presentation

PP Presentation

http://web.archive.org/web/19971017104157/www.mcnc.org/HTML/ITD/ANR/sri/index.htm